

CRYPTOLOGIA

Volume 30, No. 1, 2006

CONTENTS

The 1944 Naval BRUSA Agreement and its Aftermath	1
<i>Ralph Erskine</i>	
Alexis Köhl: A Danish Inventor of Cryptosystems	23
<i>Niels Faurholt</i>	
TELMA—A Polish Wireless Communications Security Machine of World War II	31
<i>Jan Bury</i>	
Bellaso's Reciprocal Ciphers	39
<i>Augusto Buonafalce</i>	
Note on Geheimschreiber Cam Wheels	53
<i>Deane R. Blackman</i>	
The Whirlpool Secure Hash Function	55
<i>William Stallings</i>	
Underwater Hacker Missile Wars: A Cryptography and Engineering Contest	69
<i>Joshua Holden, Richard Layton, Laurence Merkle, and Tina Hudson</i>	
Reviews and Things Cryptologic	79
<i>Louis Kruh</i>	

Volume 30, No. 2, 2006

In Memory of Jack Levine (1907–2005)	83
<i>Joel V. Brawley</i>	
The Zimmermann Telegram Revisited: A Reconciliation of the Primary Sources	98
<i>Peter Freeman</i>	
Breaking of Japanese Naval Codes: Pre-Pearl Harbor to Midway	151
<i>Forrest R. Biard</i>	
The Cycle Structure and Order of the Rail Fence Cipher	159
<i>Robert Talbert</i>	
Augmented Watermarking.	173
<i>Kiranmayi Penumarthy and Subhash Kak</i>	
Reviews and Things Cryptologic	181
<i>Louis Kruh</i>	

Volume 30, No. 3, 2006

Third Person Singular (Warsaw, 1939)	193
<i>John Gallehawk</i>	
Did Sigint Seal the Fates of 19,000 POWs?	199
<i>Lee A. Gladwin</i>	
The Indicators of Japanese Ciphers 2468, 7890, and JN-25A1	212
<i>Peter W. Donovan</i>	
Edited Transcript of Interview with Peter Hilton for "Secrets of War".	236
<i>Edited by David Joyner and David Kahn</i>	
The East German Encryption Machine T-310 and the Algorithm It Used.	251
<i>Klaus Schmeh</i>	
Solving XOR Plaintext Strings with the Viterbi Algorithm	258
<i>Alexander Griffing</i>	
Clustering and Categorization Applied to Cryptanalysis	266
<i>Claudia Oliveira, José Antônio Xexéo, and Carlos André Carvalho</i>	
Bridge Cryptography Fundamentals	281
<i>John L. Simons</i>	
Reviews and Things Cryptologic	287
<i>Louis Kruh</i>	

Volume 30, No. 4, 2006

Letter from the Editor	293
<i>Brian J. Winkel</i>	
The Poles Reveal their Secrets: Alastair Denniston's Account of the July 1939 Meeting at Pyry	294
<i>Ralph Erskine</i>	
The Cryptologic Contributions of Dr. Donald Menzel	306
<i>Craig Bauer and John Ulrich</i>	
How I Broke the Confederate Code (137 Years Too Late)	340
<i>Kent D. Boklan</i>	
Kasiski's Test: Couldn't the Repetitions be by Accident?	346
<i>Klaus Pommerening</i>	
Julius Petersen—Danish Mathematician and Cryptologist	353
<i>Augusto Buonafalce, Niels Faurholt, and Bjarne Toft</i>	

Solving the Running Key Cipher with the Viterbi Algorithm. 361
Alexander Griffing

Review of *Introduction to Coding Theory* by Ron M. Roth 368
Donald Mills

Reviews and Things Cryptologic 370
Louis Kruh

Following page 374:
Table of Contents to Volume 30
Author Index to Volume 30

Author Index To Volume 30

- Bauer, C., 306
Biard, F. R., 151
Blackman, D. R., 53
Boklan, K. D., 340
Brawley, J. V., 83
Buonafalce, A., 39, 353
Bury, J., 31

Carvalho, C. A., 266

Donovan, P. W., 212

Erskine, R., 1, 294

Faurholt, N., 23, 353
Freeman, P., 98

Gallehawk, J., 193
Gladwin, L. A., 199
Griffing, A., 258, 361

Holden, J., 69
Hudson, T., 69

Joyner, D., 236

Kahn, D., 236
Kak, S., 173
Kruh, L., 79, 181, 287, 370

Layton, R., 69

Merkle, L., 69
Mills, D., 368

Oliveira, C., 266

Penumarthi, K., 173
Pommerening, K., 346

Schmeh, K., 251
Simons, J. L., 281
Stallings, W., 55

Talbert, R., 159
Toft, B., 353

Ulrich, J., 306

Winkel, B. J., 293

Xexéo, J. A., 266

